WHAT IS CLAIMED IS:

1. A security device comprising:

a memory device comprising:

a first memory portion configured to store a device ID; and

a second memory portion configured to store a device secret;

a processor connected to the memory device, the processor configured to read the stored device ID from the first memory portion and the stored device secret from the second memory portion and perform a nonreversible computation using the stored device ID, the stored device secret, and a challenge as seeds; and

a communication circuit connected to the processor, the communication circuit configured to receive the challenge from a host device and to communicate a result of the nonreversible computation performed by the processor.

2. The security device of claim 1, wherein the memory device further comprises:

a third memory portion configured to store a service provider data item;

wherein the stored service provider data item is also used to seed the nonreversible computation.

3. The security device of claim 2, wherein the memory device further comprises:

a fourth memory portion configured to store a counter value that is incremented responsive to the service provider data item being changed;

wherein the stored counter value is also used to seed the nonreversible computation.

4. The security device of claim 1, wherein the first memory portion comprises a nonvolatile and unalterable memory device.

5. The security device of claim 4, wherein the second memory portion comprises an unalterable memory portion.

6. The security device of claim 1, wherein the communication circuit operates according to a one-wire protocol.

7. The security device of claim 1, wherein the security device is incorporated into a smart card.

8. The security device of claim 1, wherein the security device is attached to a printer cartridge.

9. The security device of claim 1, wherein the security device is incorporated into a host device.

10. The security device of claim 1, wherein the nonreversible computation is a SHA-1 computation.

11. The security device of claim 10, wherein the processor is configured to perform the SHA-1 computation serially.

12. The security device of claim 10, wherein the processor is configured to perform the SHA-1 computation in parallel.

13. A method of device authentication comprising the steps of:

receiving a challenge from a device;

generating a nonreversible computation result; and

outputting a response to the challenge, wherein the outputted response includes the nonreversible computation result;

wherein the nonreversible computation result is computed by seeding an algorithm with the received challenge, a device secret, and a unique device identifier.

14. The method of claim 13, further comprising the steps of:

generating a challenge;

transmitting the challenge to the device;

receiving a response from the device, the response including the result of the nonreversible computation, which is seeded with at least the challenge; and

authenticating the response from the device.

15. The method of claim 13, wherein the step of receiving comprises the step of:

receiving a challenge from a remote security device.

16. The method of claim 13, further comprising the steps of:

receiving the outputted response at the device; and

authenticating the received response.

17. The method of claim 15, further comprising the step of:

enabling an electronic device responsive to a positive authentication of the received response.

18. The method of claim 15, further comprising the step of:

disabling an electronic device responsive to a failure to authenticate the received response.

19. A system for device authentication, the system comprising:

a coprocessor security device configured to store a service provider data item and a device secret; and

a host device connected to the coprocessor security device, the host device configured to communicate with the coprocessor security device and a roaming security device;

wherein the roaming security device can be authenticated to thereby enable the host device.

20. The system of claim 19, further comprising:

a printer, wherein the coprocessor security device is attached to the printer.

21. The system of claim 19, further comprising a means for attaching the roaming security device to a printer cartridge.

22. The system of claim 19, further comprising:
a means for attaching the roaming security device to a printer.

23. The system of claim 20, wherein the printer cartridge is disabled responsive to the roaming security device being removed from the printer cartridge.

24. A method of device authentication, the method comprising the steps of:

receiving, at a roaming device, a challenge from a host device;

generating, at the roaming device, a nonreversible computation result, wherein the nonreversible computation result is computed by seeding a nonreversible algorithm with at least the challenge and a device secret; and

outputting to the host device a response to the challenge, wherein the outputted response includes the nonreversible computation result.

25. The method of claim 23, further comprising the steps of:

generating a challenge at the roaming device;

transmitting the challenge from the roaming device to the host device;

receiving a response from the host device, the response including the result of the nonreversible algorithm seeded with at least the challenge; and

authenticating, at the roaming device, the response from the host device.

26. The method of claim 23, further comprising the steps of:

receiving the outputted response at the host device; and

authenticating the received response at the host device.

27. The method of claim 24, further comprising the step of:

enabling an electronic device responsive to a positive authentication of the received response.

28. The method of claim 24, further comprising the step of:

disabling an electronic device responsive to a failure to authenticate the received response.

29. The method of claim 24, wherein the nonreversible computation result is computed by further seeding the nonreversible algorithm with a unique device identifier.

30. A security device comprising:

a memory device comprising a first memory portion configured to store a device secret;

a processor connected to the memory device, the processor configured to read the stored device secret from the first memory portion and to perform a hash computation using at least the stored device secret and a challenge as seeds; and

a communication circuit connected to the processor, the communication circuit configured to receive the challenge from a host device and to communicate a result of the hash computation performed by the processor.

31. The security device of claim 30, wherein the memory device is configured to store a partial secret.

32. The security device of claim 31, wherein the processor is configured to compute the device secret using the partial secret.

33. The security device of claim 30, wherein the memory device further comprises:

a second memory portion configured to store a printed page count; and

a third memory portion configured to store a maximum page count;

wherein the processor is configured to generate a signal responsive to the stored printed page count being equal to or exceeding the stored maximum page count.